

AD-A222 857

USAFA TR 90-2

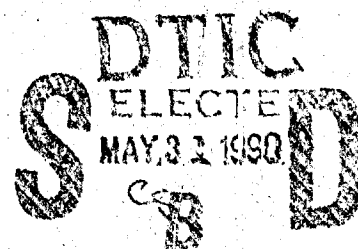
A NUMBER-THEORETIC APPROACH TO SUBGROUPS OF DIHEDRAL GROUPS

DAVID W. JENSEN, LT COL, USAF
MICHAEL K. KEANE, CAPTAIN, USAF

APRIL 1990

FINAL REPORT

APPROVED FOR PUBLIC RELEASE; DISTRIBUTION UNLIMITED



DEAN OF THE FACULTY
UNITED STATES AIR FORCE ACADEMY
COLORADO SPRINGS, CO 80840

90 05 90 063

BEST
AVAILABLE COPY

Technical Review by Major Jack J. Murphy
Department of Computer Science
USAF Academy, Colorado 80840

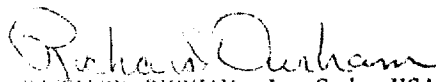
Technical Review by Capt Eric R. Bussian
Department of Mathematical Sciences
USAF Academy, Colorado 80840

Editorial Review by Lt Col Donald A. Anderson
Department of English
USAF Academy, Colorado 80840

This research report is presented as a competent treatment of the subject, worthy of publication. The United States Air Force Academy vouches for the quality of the research, without necessarily endorsing the opinions and conclusions of the authors.

This report has been cleared for open publication and/or public release by the appropriate Office of Information in accordance with AFR 190-1 and AFR 12-30. There is no objection to unlimited distribution of this report to the public at large, or by DTIC to the National Technical Information Service.

This research report has been reviewed and is approved for publication.


RICHARD DURHAM, Lt Col, USAF
Director of Research, Studies
and Analysis

Unclassified

SECURITY CLASSIFICATION OF THIS PAGE

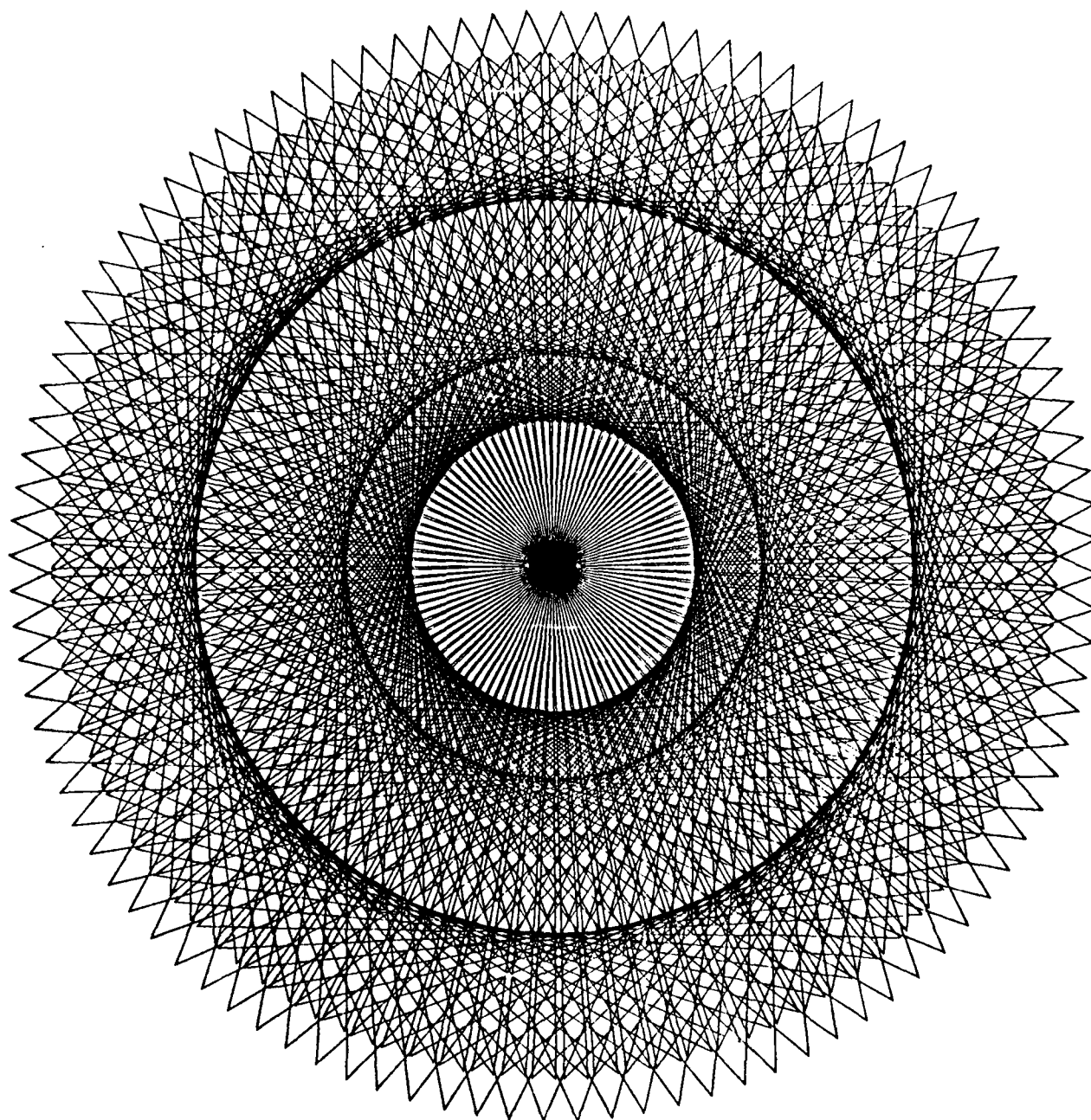
REPORT DOCUMENTATION PAGE				
1a. REPORT SECURITY CLASSIFICATION Unclassified		1b. RESTRICTIVE MARKINGS		
2a. SECURITY CLASSIFICATION AUTHORITY		3. DISTRIBUTION/AVAILABILITY OF REPORT Approved for Public Release. Unlimited Distribution.		
2b. DECLASSIFICATION/DOWNGRADING SCHEDULE		4. PERFORMING ORGANIZATION REPORT NUMBER(S)		
5a. NAME OF PERFORMING ORGANIZATION Dept of Mathematical Sciences		5b. OFFICE SYMBOL (If applicable) DFMS		5. MONITORING ORGANIZATION REPORT NUMBER(S)
6a. ADDRESS (City, State and ZIP Code) US Air Force Academy Colorado Springs, CO 80840-5701		7a. NAME OF MONITORING ORGANIZATION		
6b. ADDRESS (City, State and ZIP Code)		7b. ADDRESS (City, State and ZIP Code)		
8a. NAME OF FUNDING/SPONSORING ORGANIZATION		8b. OFFICE SYMBOL (If applicable)		9. PROCUREMENT INSTRUMENT IDENTIFICATION NUMBER
8c. ADDRESS (City, State and ZIP Code)		10. SOURCE OF FUNDING NOS.		
11. TITLE (Include Security Classification) A Number Theoretic Approach to Subgroups of Dihedral Groups		PROGRAM ELEMENT NO.	PROJECT NO.	TASK NO.
12. PERSONAL AUTHOR(S) David W. Jensen, Lt Col, USAF, and Michael K. Keane, Capt, USAF		WORK UNIT NO.		
13a. TYPE OF REPORT Final Report	13b. TIME COVERED FROM Aug 89 TO Apr 90	14. DATE OF REPORT (Yr, Mo., Day)		15. PAGE COUNT 24
16. SUPPLEMENTARY NOTATION				
17. COSATI CODES		18. SUBJECT TERMS (Continue on reverse if necessary and identify by block number)		
FIELD	GROUP	SUB. GR.		
19. ABSTRACT (Continue on reverse if necessary and identify by block number)				
<p>This report investigates the subgroup structure of dihedral groups. In Chapter I, several lemmas are presented concerning the number of subgroups of each order for a given dihedral group. The main theorem uses these lemmas to</p> <p>derive a new expression for $\sum_{k=1}^n \sigma(k)$, where $\sigma(k)$ is the sum of the positive</p> <p>divisors of k. Specifically, $\sum_{k=1}^n \sigma(k) = \sum_{k=1}^n (A_{[n/k]} - [n/2k])$, where $[x]$ denotes</p> <p>the greatest integer function, and A_i is the sequence of partial sums of $a_i =$</p> <p>$\begin{cases} 1, & i \text{ odd} \\ i+1, & i \text{ even} \end{cases}$</p> <p style="text-align: right;">(continued on reverse)</p>				
20. DISTRIBUTION/AVAILABILITY OF ABSTRACT UNCLASSIFIED/UNLIMITED <input type="checkbox"/> SAME AS RPT. <input type="checkbox"/> DTIC USERS <input type="checkbox"/>		21. ABSTRACT SECURITY CLASSIFICATION Unclassified		
22a. NAME OF RESPONSIBLE INDIVIDUAL David W. Jensen, Lt Col, USAF		22b. TELEPHONE NUMBER (Include Area Code) (719) 472-4470	22c. OFFICE SYMBOL DFMS	

Block 19:

Chapter II describes two cases where large primes, primes of the form $2^{k+1} + k$ and $2^{k+1} + 2k + 1$, relate nicely to the number of subgroups of dihedral groups. In particular, it is shown that if $T(n)$ denotes the number of subgroups of dihedral group D_n , k is a positive integer, and p is an odd prime, then (1) $T(2^k)$ is prime $\Leftrightarrow 2^{k+1} + k$ is prime and (2) $T(2^k p) = 2^{k+1} p \Leftrightarrow p = 2^{k+1} + 2k + 1$. Both results are special cases of the broader questions of when does $T(n) = 2n$ and when is $T(n)$ prime. The authors coin the term "dihedral perfect" to describe the case when $T(n) = 2n$. Chapter II also includes a simple proof that $T(n)$ is odd $\Leftrightarrow n$ is of the form $n = 2^{k_1} p_2^{k_2} \dots p_m^{k_m}$, where k_1 is odd and k_2 through k_m are even.

Accession For	
NTIS GRA&I	<input checked="" type="checkbox"/>
DTIC TAB	<input type="checkbox"/>
Unannounced	<input type="checkbox"/>
Justification	
By	
Distribution/	
Availability Codes	
Dist	Avail and/or Special
A-1	



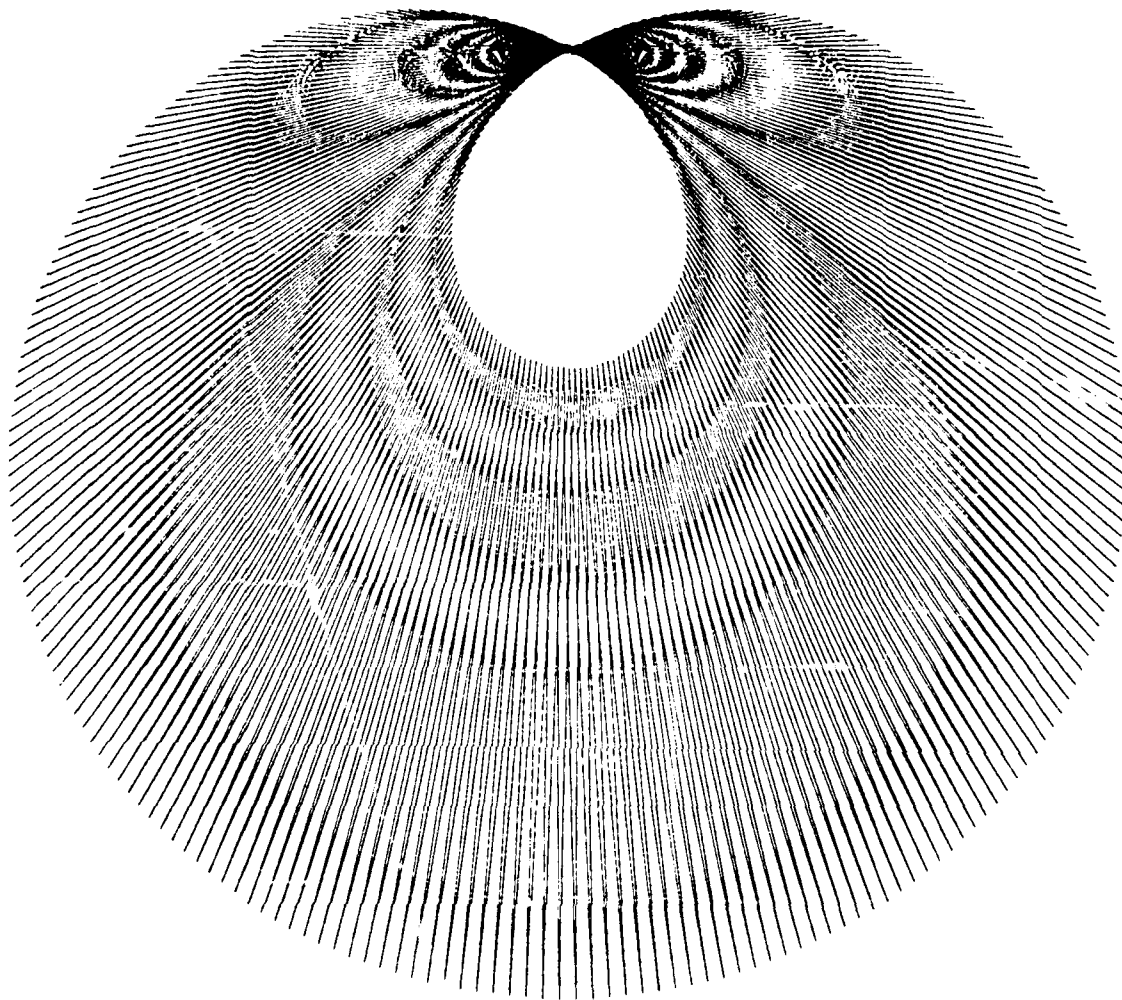


"A Number-Theoretic Approach to
Subgroups of Dihedral Groups"

DAVID W. JENSEN
MICHAEL K. KEANE

April 1990

Department of Mathematical Sciences
US Air Force Academy, CO 80840



The dihedral group on this page (D_1) and the one on the title page (D_{100}) were generated by Dr William J. Riley, RDA, Colorado Springs, Colorado, using Dr Peter Maurer's recently published algorithms [12].

TABLE OF CONTENTS

<u>CHAPTER</u>	<u>PAGE</u>
INTRODUCTION.....	1
I DIVISOR FUNCTIONS AND SUBGROUPS OF DIHEDRAL GROUPS.....	2
FOOTNOTES TO CHAPTER I.....	8
II INTRODUCING LARGE PRIMES VIA SUBGROUPS OF DIHEDRAL GROUPS.....	11
FOOTNOTES TO CHAPTER II.....	15
III OPEN QUESTIONS.....	19
IV EXTENDED BIBLIOGRAPHY.....	20

Introduction

Dihedral groups describe the symmetry of bounded figures in the plane. They are also the fundamental structures used to analyze the symmetry of more complicated objects like frieze patterns, wallpaper patterns, and three-dimensional crystals. This report investigates the subgroup structure of dihedral groups from a number theory point of view. The prerequisites needed to understand the material are modest. It is assumed that the reader is familiar with group theory and number theory at the undergraduate level.

The report presents the authors' research findings from August 1989 to March 1990. During that period, two papers were submitted for publication; they are reproduced here in chapters one and two. Footnotes have been added to clarify and expand the topics covered. Also, for those wishing to pursue the subject further, a section on open questions has been included, as well as an extended bibliography. The footnotes, open questions, and extended bibliography unify what otherwise might appear to be two disjoint papers. (KR) ←

As a final note, the authors would like to thank Mr Tim Whalen for superbly typing the original manuscript, and then persevering through several revisions.

Divisor Functions and Subgroups of Dihedral Groups

A picture can really be worth a thousand words. For example, consider Figure 1 which depicts the number of subgroups of every order for dihedral group D_n , $n = 1, 2, 3, \dots, 20$.¹ The total number of subgroups of D_n , denoted $T(n)$, is also shown. The most striking feature of the table is its numerous patterns and symmetries. Taken together, these patterns highlight the rich structure of dihedral groups in a way that would be hard to duplicate using words. This article looks at the subgroup structure of dihedral groups, using Figure 1 to guide the discussion. Several familiar facts are reviewed, and a new expression for $\sum_{k=1}^n \sigma(k)$, where $\sigma(k)$ is the sum of the positive divisors of k , is presented. Figure 1 comes from a computer program the authors created to list elements, subgroups, and various properties for certain classes of finite groups.²

Dihedral groups are easy to define, and they are familiar to most undergraduate math majors. Less well-known, however, is the extent to which they illustrate the beautiful interplay between abstract algebra and number theory. Before gleaning what Figure 1 has to offer, let's review a few simple facts that will be needed in the sequel. A dihedral group D_n has order $2n$, and is most easily understood as the group of symmetries of a regular n -gon. In this context D_n contains C_n , the cyclic group of n rotations. Since C_n is isomorphic to Z_n , C_n has $\tau(n)$ subgroups, where $\tau(n)$ is the number of positive divisors of n . All the other subgroups of D_n , including D_n itself, consist of an equal number of reflections and rotations, and they therefore have even order. Finally, for every divisor t of n , there are exactly n/t subgroups of order $2t$ that contain both reflections and rotations.³

The Number of Subgroups of $D(n)$

$D(n)$	$T(n)$	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20
$D(20)$	48	1	21	11	1				5		5										3
$D(19)$	22	1	19																	1	
$D(18)$	45	1	19	1	9		7		1		3								3		
$D(17)$	20	1	17															1			
$D(16)$	36	1	17		9				5								3				
$D(15)$	28	1	15	1		1	5			3						1					
$D(14)$	28	1	15		7			1							3						
$D(13)$	16	1	13										1								
$D(12)$	34	1	13	1	7		5		3					3							
$D(11)$	14	1	11										1								
$D(10)$	22	1	11		5	1				3											1
$D(9)$	16	1	9	1			3		1										1		
$D(8)$	19	1	9		5				3									1			
$D(7)$	10	1	7					1							1						
$D(6)$	16	1	7	1	3		3						1								
$D(5)$	8	1	5			1					1										
$D(4)$	10	1	5		3				1												
$D(3)$	6	1	3	1			1														
$D(2)$	5	1	3			1															
$D(1)$	2	1	1																		

FIGURE 1

Note that Figure 1 supports the following important fact:

The total number of subgroups of a dihedral group D_n is given by the summatory function [1]:

$$T(n) = \sum_{m|n} (m+1) = \sigma(n) + \tau(n).$$

With a little extra probing, Figure 1 also points to other fascinating results. In particular, note the way the sequence $a_i = 1, 3, 3, 5, 5, 7, 7, \dots$ repeats itself vertically at every even order. This sequence lies at the heart of our main theorem. To get to it we first need several short lemmas, each of which is interesting in its own right.

Lemma 1. In a dihedral group, there never exists more than one subgroup of order k when k is odd.

Proof: Let D_n be a dihedral group. Only the odd ordered subgroups of C_n need be considered since all other subgroups of D_n have even order. The result follows by simply noting that C_n is isomorphic to Z_n , and Z_n never has more than one subgroup of any given order. \square

Lemma 2. The number of subgroups m of a given order k in a dihedral group is either zero or odd.

Proof: Lemma 1 takes care of the case when k is odd. If k is even and $m \neq 0$, then $k|2n$, and moreover, $k/2|n$. Therefore, there are exactly $2n/k$ subgroups of order k that contain both reflections and rotations.

- Case 1. If $2n/k$ is even, then $k|n$ and there is also a cyclic subgroup of order k . Therefore $m = (2n/k) + 1$ is odd.

- Case 2. If $2n/k$ is odd, then $k \nmid n$ and there is no cyclic subgroup of order k . Then $m = 2n/k$ is again odd. \square

Lemma 3. Assume m is a positive odd integer and k is a positive even integer. Then dihedral group D_n contains precisely m subgroups of order k if and only if $n = mk/2$ or $n = (m-1)k/2$.

Proof: Assume first that D_n contains precisely m subgroups with even order k . We arrive at the desired conclusion by noting that the proof of Lemma 2 implies $m = 2n/k + 1$ or $m = 2n/k$.

If we start by assuming $n = (m-1)k/2$, then $(k/2) \mid n$ and there are $2n/k = m-1$ subgroups of order k that have both reflections and rotations. Since $m-1$ is even, Lemma 2 implies a cyclic subgroup of order k must also exist. Therefore, the total number of subgroups of order k must be m . Using similar arguments, $n = mk/2$ also implies there are m subgroups of order k . \square

Several corollaries follow immediately from Lemma 3.⁴ For example, if $m \geq 3$, then the smallest dihedral group having precisely m subgroups of order k_1 , and m subgroups of order k_2 , $k_1 \neq k_2$, is $D_{(m^2-m)}$. Figure 1 nicely illustrates this fact for $m = 3$ and $m = 5$. Lemma 3 is also useful in establishing our main theorem. In what follows, let $T_e(n)$ and $T_o(n)$ denote the number of even and odd ordered subgroups contained in D_n , respectively. Also assume $[x]$ represents the largest integer not exceeding x , and a_i is the sequence previously mentioned, that is

$$a_i = \begin{cases} i, & i \text{ odd} \\ i+1, & i \text{ even.} \end{cases}$$

Lemma 4. $\sum_{k=1}^n T_o(k) = \sum_{k \text{ odd}}^n [n/k]$

Proof: From Lemma 1 we know a dihedral group D_n can have at most one cyclic subgroup of odd order k . Moreover, a cyclic subgroup of order k exists if and only if $k|n$. Thus the number of subgroups of odd order k embedded in the dihedral groups with order $\leq 2n$ equals the number of times it is true that k divides r for $r = 1, 2, 3, \dots, n$. This in turn equals $[n/k]$. Therefore, the total number of subgroups of odd order embedded in the dihedral groups with order $\leq 2n$ is $\sum_{k \text{ odd}}^n [n/k]$. \square

Lemma 5. $\sum_{j=1}^n T_e(j) = \sum_{j=1}^n A_{[n/j]}$, where A_i is the sequence of partial sums of a_i .

Proof: Let k be an even integer. From Lemma 3, there is only one dihedral group that contains exactly one subgroup of order k , namely $D_{k/2}$. For $m = 3, 5, 7, \dots$, the dihedral groups that contain precisely m subgroups of order k are $D_{mk/2}$ and $D_{(m-1)k/2}$. Therefore all the dihedral groups that contain subgroups with order k are given by $D_{i(k/2)}$, $i = 1, 2, 3, \dots$. Moreover, the number of subgroups of order k in $D_{i(k/2)}$ is a_i . This implies that the number of subgroups of even order k embedded in the dihedral groups with order $\leq 2n$

is $\sum_{i=1}^{[2n/k]} a_i$. We conclude that $\sum_{j=1}^n T_e(j)$, the total number of even ordered subgroups embedded in the dihedral groups with order $\leq 2n$, equals

$$\sum_{k \text{ even}}^{2n} \sum_{i=1}^{[2n/k]} a_i. \quad \text{Then} \quad \sum_{k \text{ even}}^{2n} \sum_{i=1}^{[2n/k]} a_i = \sum_{k=1}^n \sum_{i=1}^{[n/k]} a_i = \sum_{k=1}^n A_{[n/k]},$$

where A_i is the sequence of partial sums of a_i . \square

Theorem. $\sum_{k=1}^n \sigma(k) = \sum_{k=1}^n (A_{[n/k]} - [n/2k]).^5$

Proof: From (1) we have $\sum_{k=1}^n T(k) = \sum_{k=1}^n (\sigma(k) + \tau(k))$, and from Lemmas 4 and 5

we have $\sum_{k=1}^n T(k) = \sum_{k=1}^n A_{[n/k]} + \sum_{k \text{ odd}}^n [n/k]$. It is also true that

$\sum_{k=1}^n \tau(k) = \sum_{k=1}^n [n/k]$, [2].⁶ We therefore conclude that

$$\sum_{k=1}^n \sigma(k) = \sum_{k=1}^n A_{[n/k]} + \sum_{k \text{ odd}}^n [n/k] - \sum_{k=1}^n [n/k] = \sum_{k=1}^n A_{[n/k]} - \sum_{k \text{ even}}^n [n/k]$$

$$= \sum_{k=1}^n A_{[n/k]} - \sum_{k=1}^n [n/2k] = \sum_{k=1}^n (A_{[n/k]} - [n/2k]). \quad \square$$

As an example of how the theorem works, let $n = 5$.

$$\text{Then } \sum_{k=1}^5 \sigma(k) = (1) + (1+2) + (1+3) + (1+2+4) + (1+5) = 21,$$

$$\begin{aligned} \text{and } \sum_{k=1}^5 (A_{[5/k]} - [5/2k]) &= (A_5 + A_2 + A_1 + A_1 + A_1) - (2+1) \\ &= (17 + 4 + 1 + 1 + 1) - (3) = 21. \end{aligned}$$

Footnotes to Chapter 1

1. Figure 2 on page 9 extends Figure 1 by depicting the number of subgroups of each order for dihedral group D_n , $21 \leq n \leq 40$. As in the top half of Figure 1, the trivial subgroup consisting of D_n itself is included in $T(n)$, but not shown on the graph.
2. A detailed description of the computer program used to generate Figures 1 and 2 will be published as a separate US Air Force Academy Technical Report.
3. The simple facts about dihedral groups referenced on page 2 can be verified in references [1] and [3] of the extended bibliography.
4. The following corollaries also follow immediately from Lemma 3:

Corollary 1 Assume m is a positive odd integer, $m \geq 3$. Then \exists a dihedral group with exactly m subgroups of order k_1 , m subgroups of order k_2 , and m subgroups of order k_3 , where k_1 , k_2 , and k_3 are distinct.

Sketch of Proof Refer to Lemma 3 and note that for n and m fixed, the equations $n = m \left(\frac{k}{2}\right)$ and $n = (m-1) \left(\frac{k}{2}\right)$ yield at most two distinct solutions.

Corollary 2 Assume m is a positive odd integer, $m \geq 3$. Let K_n be the number of dihedral groups of order $\leq 2n$, each of which has precisely m subgroups of the same order. Then $K_n = \left\lfloor \frac{n}{m} \right\rfloor + \left\lfloor \frac{n}{m-1} \right\rfloor - \left\lfloor \frac{n}{m(m-1)} \right\rfloor$.

Sketch of Proof: The only time we can get m subgroups of a given order in dihedral group D_t is when m or $(m-1)$ divides t . For $t = 1, 2, \dots, n$, the number of times m divides t is given by $\left\lfloor \frac{n}{m} \right\rfloor$, and the number of times $m-1$ divides t is given by $\left\lfloor \frac{n}{m-1} \right\rfloor$. The term $\left\lfloor \frac{n}{m(m-1)} \right\rfloor$ takes care of the "overlap", where both m and $m-1$ divide t .

The number of Subgroups of $D(n)$

$D(n)$	96	41	21	1	11	9	5	5	5	3
$D(40)$	96	41	21	1	11	9	5	5	5	3
$D(39)$	60	39	1	13	1				3	
$D(38)$	64	39	19				1			3
$D(37)$	40	37								1
$D(36)$	160	37	19	13	9	1	7	5	3	3
$D(35)$	52	35	1	1	7		5			1
$D(34)$	58	35	17					1		3
$D(33)$	52	33	1	11	1			3		1
$D(32)$	69	33	17		9		5		3	
$D(31)$	34	31							1	
$D(30)$	80	31	15	11	7	5	1	3		3
$D(29)$	32	29							1	
$D(28)$	62	29	15	1	7		5		3	
$D(27)$	44	27	1	9	1		3		1	
$D(26)$	46	27	13			1			3	
$D(25)$	34	25	1		5			1		
$D(24)$	66	25	13	9	7	5	3			3
$D(23)$	26	23						1		
$D(22)$	40	23	11		1			3		
$D(21)$	36	21	1	7	1		3		1	
$\Sigma(n)$										

1 2 3 4 5 6 7 8 9 10 11 12 13 14 15 16 17 18 19 20 21 22 23 24 25 26 27 28 29 30 31 32 33 34 35 36 37 38 39 40

Order of Subgroups

FIGURE 2

5. It is well-known that the sequence of positive odd integers $C_i = (2i - 1)$ yields $\sum_{i=1}^n C_i = n^2$. Using this it is easy to show that A_i can be expressed as follows:

$$A_i = \begin{cases} \frac{i^2 + 1}{2} & , i \text{ even} \\ \frac{i^2 + 2i - 1}{2} & , i \text{ odd} . \end{cases}$$

With this expression for A_i , different formulations of the main theorem are possible. However, none are as concise as the one given.

6. In addition to the fact that $\sum_{k=1}^n \tau(k) = \sum_{k=1}^n \left[\frac{n}{k} \right]$, it is also common knowledge that $\sum_{k=1}^n \sigma(k) = \sum_{k=1}^n k \left[\frac{n}{k} \right]$. A good reference for these, as well as hundreds of other statements about arithmetic functions, is Dickson's "History of the Theory of Numbers," [2].

Introducing Large Primes via Subgroups of Dihedral Groups

For both the novice and the seasoned mathematician, Fermat primes and Mersenne primes are an endless source of enjoyment and speculation. Fermat primes¹ are primes of the form $F_m = 2^{2^m} + 1$ where m is a nonnegative integer, and Mersenne primes² are primes of the form $M_p = 2^p - 1$ where p is itself a prime number. This paper shows that similar large primes are also important for understanding the structure of dihedral groups. In particular, simple examples are given where large primes, primes of the form $2^{k+1} + k$ and primes of the form $2^{k+1} + 2k + 1$, relate nicely to the number of subgroups of dihedral groups.

Stephen Cavior has shown that the number of subgroups of dihedral group D_n , denoted $T(n)$, is given by $T(n) = \sum_{m|n} (m + 1) = \sigma(n) + \tau(n)$, where $\tau(n)$ is the number of positive divisors of n and $\sigma(n)$ is the sum of those divisors [1].³ For example, for $n = 6$ we have $T(n) = (1 + 2 + 3 + 6) + 4 = 16$. Three questions about $T(n)$ naturally arise:

- When is $T(n)$ odd?
- When is $T(n)$ prime?
- When does $T(n) = 2n$?

The first question is easily answered by our Lemma 1. The second and third questions give rise to the search for large primes of the kind alluded to earlier. The question of when $T(n)$ equals $2n$ is especially appealing. In terms of Group Theory, it is equivalent to asking when the order of a dihedral group equals the number of its subgroups. From a Number Theory perspective, it is a fascinating extension to the search for perfect numbers, numbers which satisfy $\sigma(n) = 2n$. In the sequel we shall refer to the following well-known

facts for $n = p_1^{k_1} p_2^{k_2} \dots p_m^{k_m}$ in standard form [2]:⁴

$$(1) \quad \tau(n) = \prod_{i=1}^m (k_i + 1)$$

$$(2) \quad \sigma(n) = \prod_{i=1}^m \frac{p_i^{k_i+1} - 1}{p_i - 1} = \prod_{i=1}^m (p_i^{k_i} + p_i^{k_i-1} + \dots + p_i + 1)$$

Lemma 1. $T(n)$ is odd if and only if n is of the form $n = 2^{k_1} p_2^{k_2} p_3^{k_3} \dots p_m^{k_m}$, where k_1 is odd and k_2 through k_m are even.

Proof: It follows easily from (1) and (2) that for $n = 2^{k_1} p_2^{k_2} \dots p_m^{k_m}$,

(3) $\tau(n)$ is odd $\Leftrightarrow n$ has only even powers of primes.

(4) $\sigma(n)$ is odd $\Leftrightarrow n$ has only even powers of odd primes.

Notice that (3) and (4) imply that if $\tau(n)$ is odd, then $\sigma(n)$ must also be odd. Therefore we may conclude that $T(n) = \sigma(n) + \tau(n)$ is odd if and only if $\sigma(n)$ is odd and $\tau(n)$ is even. Again using (3) and (4), this can only happen when $p_1 = 2$, k_1 is odd, and k_2 through k_m are even. \square

Lemma 1 points us in the right direction when we consider our second question. That is, which dihedral groups have a prime number of subgroups? Note that for $n = 1$ we have $T(n) = T(1) = 2$, a prime. All other $T(n)$ prime are odd numbers, and for each one, n must be of the form given in Lemma 1. Therefore the easiest place to look for $T(n)$ to be prime is among n of the form $n = 2^k$, k odd. Using (1) and (2), $T(2^k)$ is prime if and only if $\sigma(2^k) + \tau(2^k) = (2^{k+1} - 1) + (k + 1) = 2^{k+1} + k$ is prime. We therefore have the following theorem:

Theorem 2. If k is a positive integer, then

$$T(2^k) \text{ is prime} \Leftrightarrow 2^{k+1} + k \text{ is prime.}$$

Of course, the real fun begins in trying to actually find the odd positive integers k for which $2^{k+1} + k$ is prime. Using a computer package like "Derive," it is easy to show that the only values of k less than 200 for which $2^{k+1} + k$ is prime are $k = 1, 3, 7, 9, 15$, and 85 . It is interesting to note that $k = 85$ yields the behemoth $T(2^{85}) = 77371252455336267181195349$, a prime! It is also true that $T(n)$ may be prime for n in the more general form $n = 2^{k_1} p_2^{k_2} p_3^{k_3} \dots p_m^{k_m}$, where k_2 through k_m can be nonzero even integers. As a quick example, it follows from (1) and (2) that $n = 2 \cdot 3^4 = 162$ yields the prime $T(162) = \sigma(162) + \tau(162) = 373$.

We now turn our attention to the third question posed at the outset. Namely, which n yield $T(n) = 2n$? We shall call such numbers "dihedral perfect," and we can make several immediate observations. Since $T(p) = \sigma(p) + \tau(p) = (p + 1) + 2 = p + 3$ whenever p is prime, it is clear that the only dihedral perfect prime is $p = 3$. Using (1) and (2), it is also clear that for $n = 2^k$ we have $T(n) = T(2^k) = \sigma(2^k) + \tau(2^k) = (2^{k+1} - 1) + (k + 1) = 2^{k+1} + k$. Thus $n = 2^k$ is dihedral perfect, that is $T(2^k) = 2^{k+1}$, if and only if $k = 0$. A logical next step is to ask if there are dihedral perfect numbers of the form $n = 2^k p$, which brings us to our final theorem.

Theorem 3. If $n = 2^k p$ where k is a positive integer and p is an odd prime, then

$$T(n) = 2n \Leftrightarrow p = 2^{k+1} + 2k + 1.$$

Proof: The proof is simple and we again use (1) and (2) to establish:

$$n = 2^k p \text{ is dihedral perfect} \Leftrightarrow (2^{k+1} - 1) \left(\frac{p^2 - 1}{p - 1} \right) + (k + 1)(2) = 2^{k+1} p$$

$$\Leftrightarrow (2^{k+1} - 1)(p + 1) + 2(k + 1) = 2^{k+1} p$$

$$\Leftrightarrow p = 2^{k+1} + 2k + 1. \quad \square$$

Therefore asking when $n = 2^k p$ is dihedral perfect is equivalent to searching for primes of the form $2^{k+1} + 2k + 1$. The values of k , $1 \leq k \leq 200$, for which $2^{k+1} + 2k + 1$ is prime are $k = 1, 2, 3, 4, 7, 10, 13, 14, 26, 40, 49, 50, 110, 142$, and 170 . For $k = 170$, the dihedral perfect number $n = 2^k p = 2^k (2^{k+1} + 2k + 1)$ has 103 digits! As a final note, there exist dihedral perfect numbers besides the ones mentioned above, a simple example being $n = 2 \cdot 5 \cdot 13 = 130$.⁵

Footnotes to Chapter II

1. Numbers of the form $F_m = 2^{2^m} + 1$ are called Fermat numbers. The first five Fermat numbers, $F_0 = 3$, $F_1 = 5$, $F_2 = 17$, $F_3 = 257$, and $F_4 = 65537$ are all prime. Although Fermat conjectured that this trend would continue, Leonard Euler showed that F_5 is composite. Indeed, at present no other Fermat primes have been discovered. The smallest Fermat number whose primality status remains unknown is F_{14} [16].

2. Perfect numbers and Mersenne primes are closely linked as follows:

$$n \text{ is an even perfect number if and only if } n = 2^{p-1} M_p$$

where M_p is a Mersenne prime.

(The "if" portion of the statement was known by Euclid; the "only if" part was established by Euler.)

There are only 31 known Mersenne primes. Therefore there are only 31 known even perfect numbers. The existence of odd perfect numbers is still an open question. Table 1 on page 17 lists the known Mersenne primes and is reproduced from Rosen's text. [15].

3. Table 2 on page 18 gives the values of $\tau(n)$, $\sigma(n)$, and $T(n)$ for $1 \leq n \leq 100$. It was created using information from Rosen's book [15].

4. The Fundamental Theorem of Arithmetic states that each integer greater than 1 can be written as a product of primes, and, except for the order in which these are written, this can be done in only one way [3]. By arranging the prime factors of n in increasing order, we obtain the unique standard form of n :

$$n = p_1^{k_1} p_2^{k_2} \dots p_m^{k_m} \text{ where } p_1 < p_2 < \dots < p_m.$$

5. Two more results concerning dihedral perfect numbers are given below:

Lemma 1 There are no dihedral perfect numbers of the form $n = p^2$, where p is prime.

Sketch of Proof: The lemma is true if $p = 2$. Therefore assume p is odd. If $n = p^2$, then n is dihedral perfect $\Leftrightarrow \frac{p^2 - 1}{p - 1} + 3 = 2p^2 \Leftrightarrow p^3 - 2p^2 - 3p + 4 = 0$. We conclude n cannot be dihedral perfect since a rational root (and therefore a prime root) of the above polynomial must divide 4.

Lemma 2 There are no dihedral perfect numbers of the form $n = p_1 p_2$, where p_1 and p_2 are odd primes.

Sketch of Proof: If $n = p_1 p_2$ was dihedral perfect we would have $(p_1 + 1)(p_2 + 1) + 4 = 2p_1 p_2$, which implies $p_1 p_2 = p_1 + p_2 + 5$. No odd primes can satisfy this last expression.

p	Number of decimal digits in M_p	Date of Discovery
2	1	ancient times
3	1	ancient times
5	2	ancient times
7	3	ancient times
13	4	Mid 15th century
17	6	1603
19	6	1603
31	10	1772
61	19	1883
89	27	1911
107	33	1914
127	39	1876
521	157	1952
607	183	1952
1279	386	1952
2203	664	1952
2281	687	1952
3217	969	1957
4253	1281	1961
4423	1332	1961
9689	2917	1963
9941	2993	1963
11213	3376	1963
19937	6002	1971
21701	6533	1978
23209	6987	1979
44497	13395	1979
86243	25962	1983
132049	39751	1983
110503	33265	1988
216091	65050	1985

Table 1. The Known Mersenne Primes.

n	$\tau(n)$	$\sigma(n)$	T(n)
1	1	1	2
2	2	3	5
3	2	4	6
4	3	7	10
5	2	6	8
6	4	12	16
7	2	8	10
8	4	15	19
9	3	13	16
10	4	18	22
11	2	12	14
12	6	28	34
13	2	14	16
14	4	24	28
15	4	24	28
16	5	31	36
17	2	18	20
18	6	39	45
19	2	20	22
20	6	42	48
21	4	32	36
22	4	36	40
23	2	24	26
24	8	60	68
25	3	31	34
26	4	42	46
27	4	40	44
28	6	56	62
29	2	30	32
30	8	72	80
31	2	32	34
32	6	63	69
33	4	48	52
34	4	54	58
35	4	48	52
36	9	91	100
37	2	38	40
38	4	60	64
39	4	56	60
40	8	90	98
41	2	42	44
42	8	96	104
43	2	44	46
44	6	84	90
45	6	78	84
46	4	72	76
47	2	48	50
48	10	124	134
49	3	57	60
50	6	93	99

n	$\tau(n)$	$\sigma(n)$	T(n)
51	4	72	76
52	6	98	104
53	2	54	56
54	8	120	128
55	4	72	76
56	8	120	128
57	4	80	84
58	4	90	94
59	2	60	62
60	12	168	180
61	2	62	64
62	4	96	100
63	6	104	110
64	7	127	134
65	4	84	88
66	8	144	152
67	2	68	70
68	6	126	132
69	4	96	100
70	8	144	152
71	2	72	74
72	12	195	207
73	2	74	76
74	4	114	118
75	6	124	130
76	6	140	146
77	4	96	100
78	8	168	176
79	2	80	82
80	10	186	196
81	5	121	126
82	4	126	130
83	4	84	86
84	12	224	236
85	4	108	112
86	4	132	136
87	4	120	124
88	8	180	188
89	2	90	92
90	12	234	246
91	4	112	116
92	6	168	174
93	4	128	132
94	4	144	148
95	4	120	124
96	12	252	264
97	2	98	100
98	6	171	177
99	6	156	162
100	9	217	226

Table 2

Open Questions

1. Do there exist odd dihedral perfect numbers other than 1 and 3?
2. Do there exist dihedral perfect numbers of the form $n = p^k$, where p is an odd prime and k is greater than 2?
3. Do there exist dihedral perfect numbers of the form $n = p_1 p_2 \dots p_k$ where all the p_i 's are odd primes and $k \geq 3$?
4. Under what circumstances do we get $T(n) = T(m)$, $n \neq m$? (It first occurs for $T(4) = T(7) = 10$. An early stunning example is $T(36) = T(62) = T(69) = T(77) = T(97) = 100$.)
5. Do there exist positive integers n and m , $n \neq m$, such that $T(n) = T(m) =$ an odd integer?
6. Under what circumstances do we get "amicable" dihedral numbers; that is, when do distinct positive integers satisfy $T(n) = T(m) = n + m$?
7. How rare are dihedral triperfect numbers; that is, when does n satisfy $T(n) = 3n$? (The first dihedral triperfect number is $n = 60$.)
8. The Erdos-Sierpinski Conjecture suggests there are an infinite number of solutions to $\sigma(n) = \sigma(n + 1)$. Are there an infinite number of solutions to $T(n) = T(n + 1)$? (It first occurs for $T(14) = T(15) = 28$.)

Extended Bibliography

1. Cavior, S.R., "The Subgroups of the Dihedral Groups", Mathematics Magazine, 48 (1975), 107.
2. Dickson, L.E., History of the Theory of Numbers, Vol I, Chelsea, New York, 1952.
3. Durbin, J.R., Modern Algebra: an Introduction, 2nd ed., Wiley, New York, 1985.
4. Gallian, J.A., Contemporary Abstract Algebra, 2nd ed., D.C. Heath and Company, Massachusetts, 1990.
5. Guy, R.K., Reviews in Number Theory 1973-83, Vol 1A, American Mathematical Society, Rhode Island, 1984.
6. Jensen, D.W., "Plane Symmetry Groups", Chapter 1 of "Symmetry in the Basic Sciences", USAF Academy Technical Report, 89-3, April 1989.
7. Jensen, D.W., and Keane, M.K., "Divisor Functions and Subgroups of Dihedral Groups", submitted.
8. Jensen, D.W., and Keane, M.K., "Introducing Large Primes via Subgroups of Dihedral Groups", submitted.
9. Keane, M.K., The Personal Computer as an Aid in the Study of Group Theory, Masters Thesis, The American University, University Microfilms International, Michigan, 1985.
10. Keane, M.K., and Jensen, D.W., "The Personal Computer and Group Theory", to appear.
11. Leveque, W.J., Reviews in Number Theory, 1940-72, Vol 1, American Mathematical Society, Rhode Island, 1974.
12. Maurer, P.M., "A Rose is a Rose", American Mathematical Monthly, 94 (1987), 631-645.

13. Ore, O., Number Theory and its History, Dover republication (1988) of McGraw-Hill edition, New York, 1948.
14. Riesel, H., Prime Numbers and Computer Methods for Factorization, revised 2nd printing, Birkhauser, Boston, 1987.
15. Rosen, K.H., Elementary Number Theory and its Application, 2nd ed., Addison-Wesley, Massachusetts, 1988.
16. Schroeder, M.R., Number Theory in Science and Communication, 2nd ed., Springer-Verlag, New York, 1986.